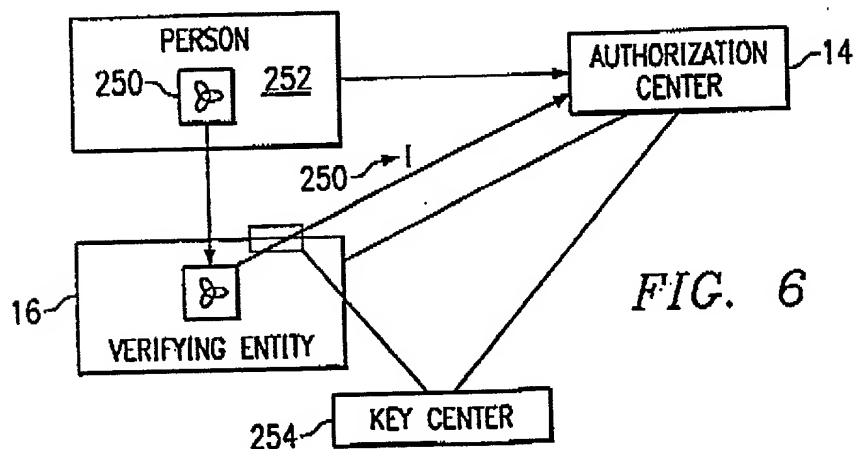
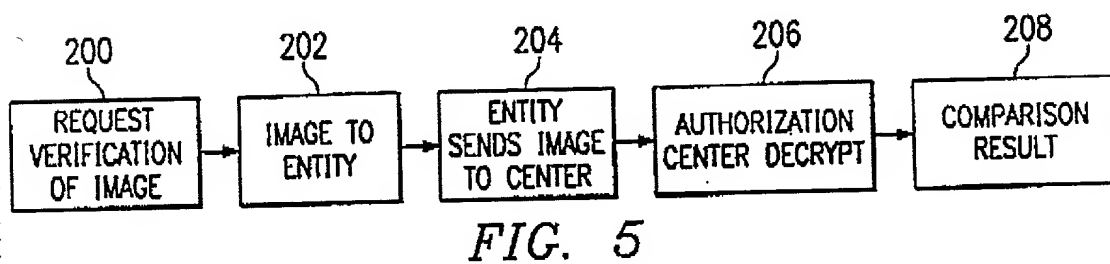
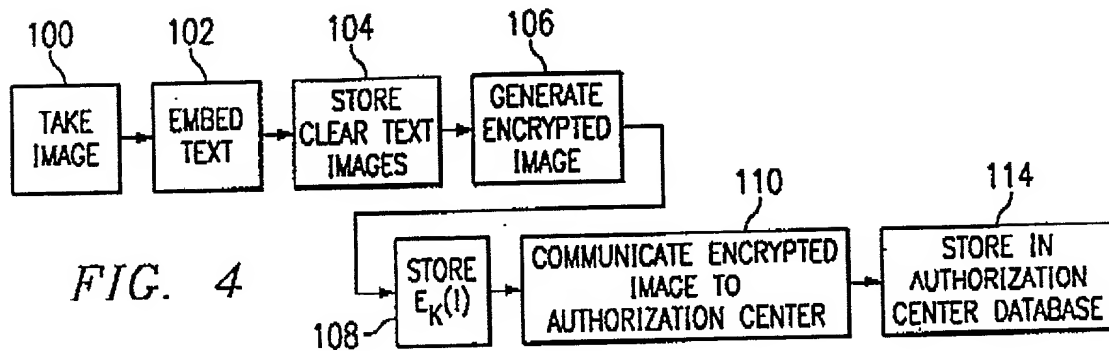


FIG. 2



METHOD AND SYSTEM FOR DIGITAL IMAGE AUTHENTICATION CENTER

Inventor: Jon W. Hamilton (Page 4 of 19)
Express Mail Label EL 926775935 US 021971.0165

FIG. 7

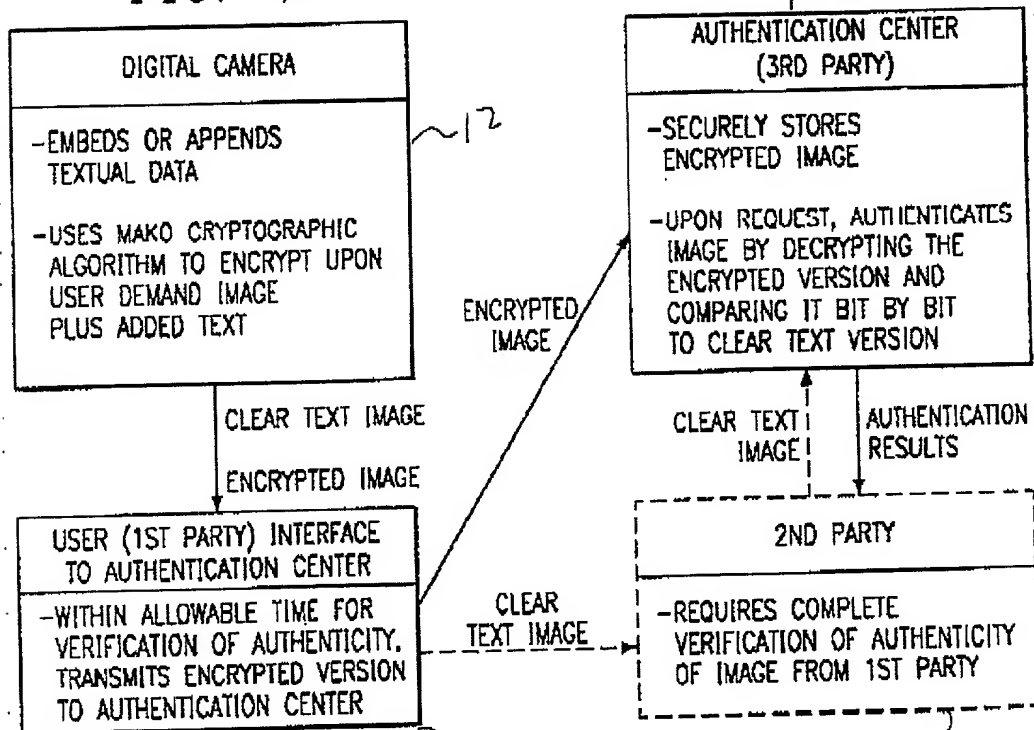
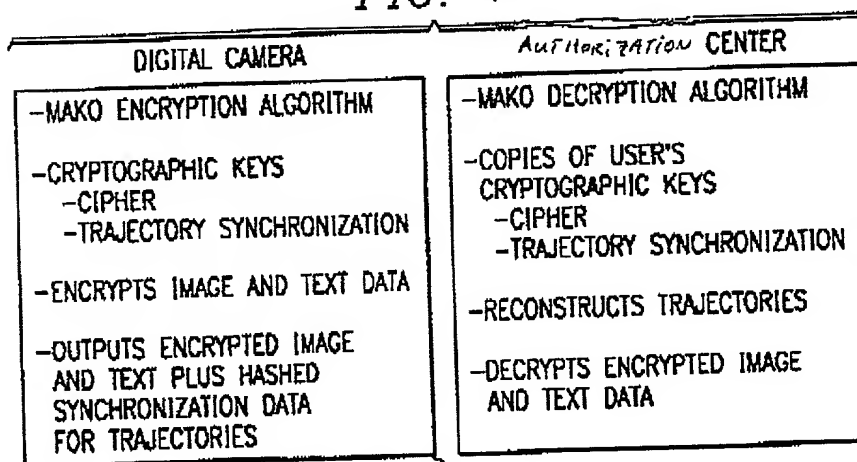
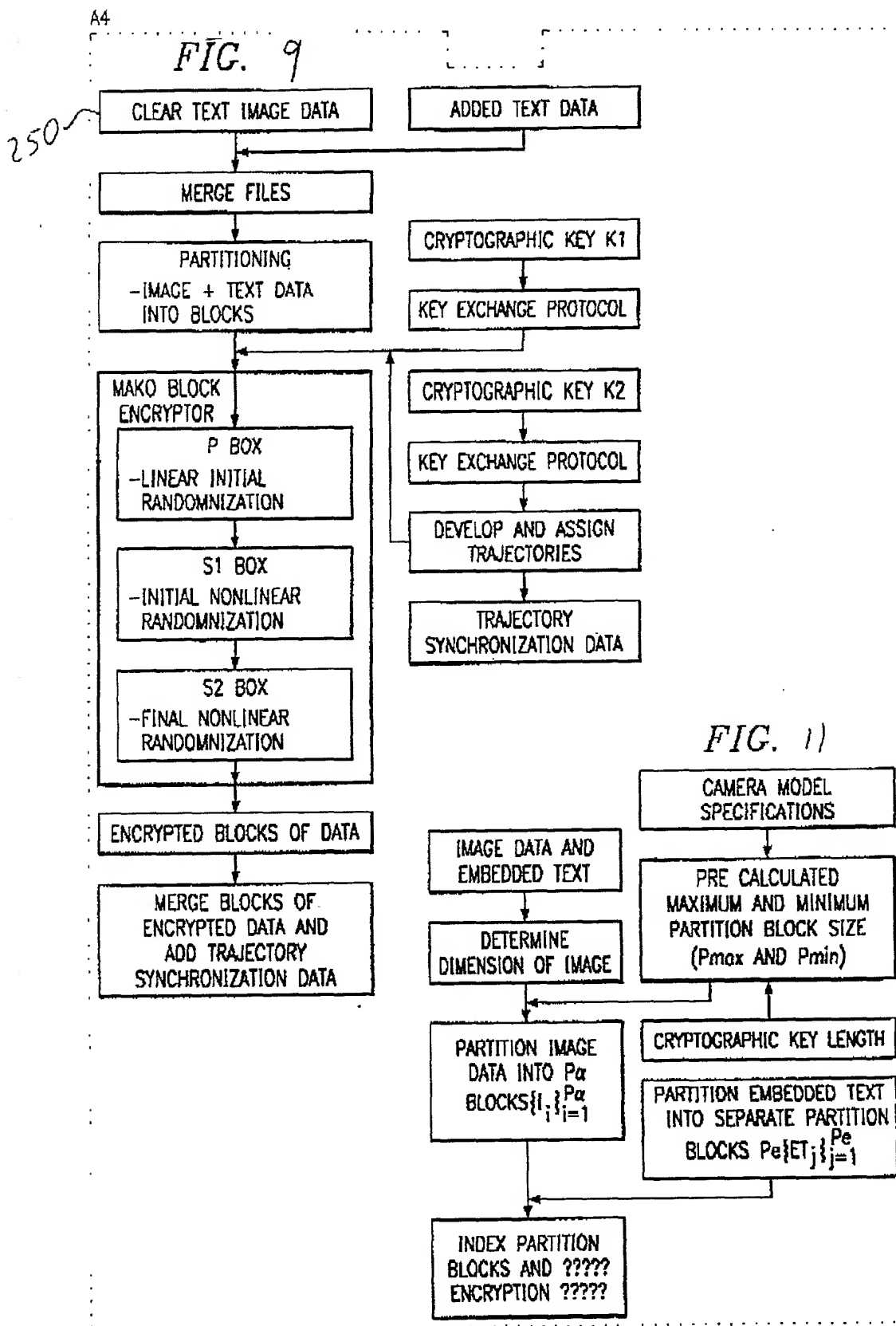


FIG. 8

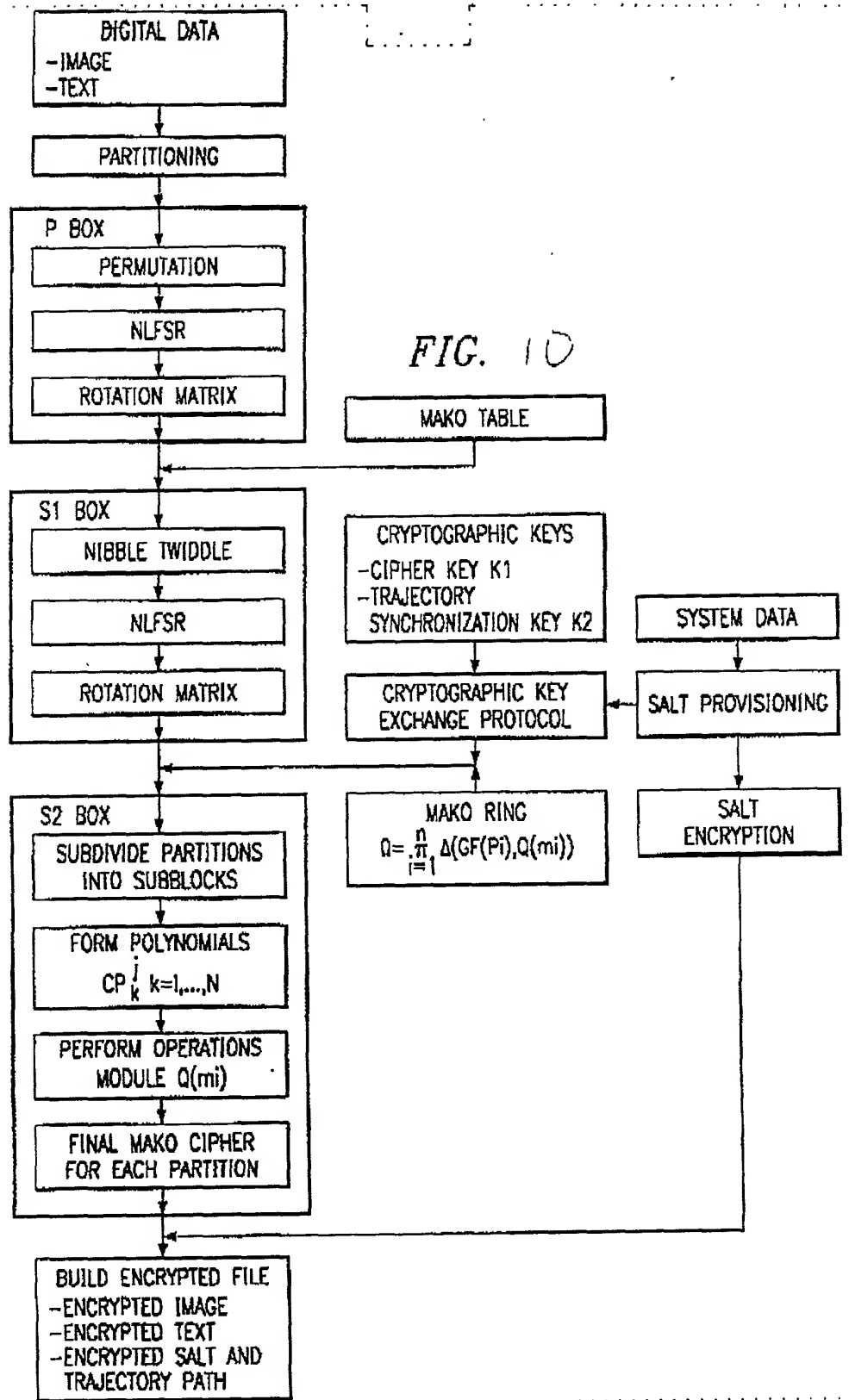




METHOD AND SYSTEM FOR DIGITAL IMAGE AUTHENTICATION CENTER

Inventor: Jon W. Hamilton (Page 6 of 19)
Express Mail Label EL 926775935 US 021971.0165

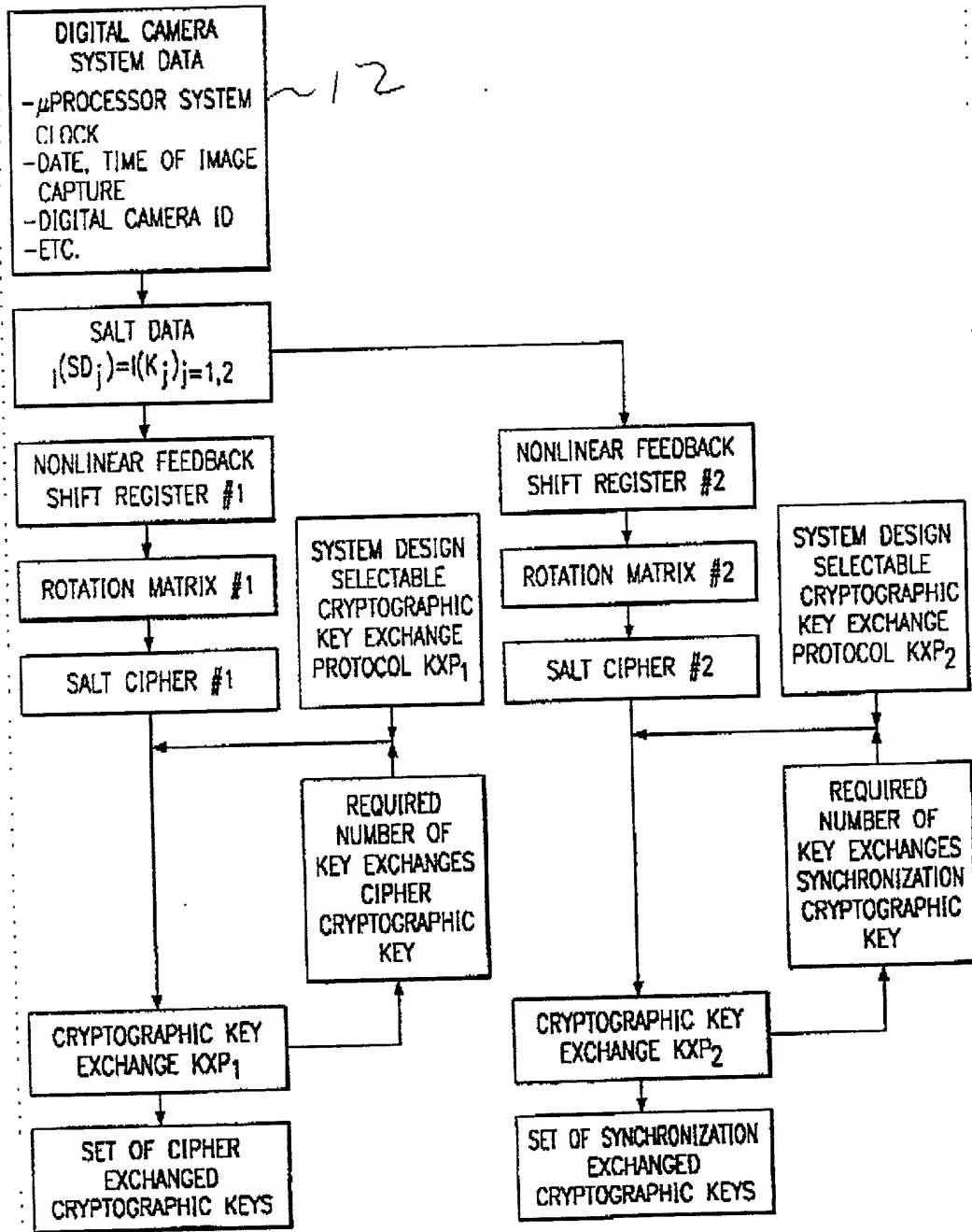
A4



10026344.436104

A4

FIG. 12



1003341-1003341

A4

FIG. 13

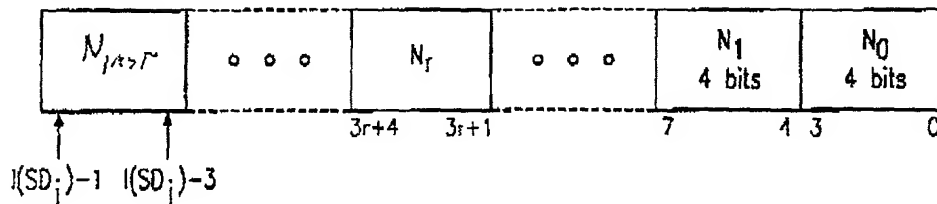
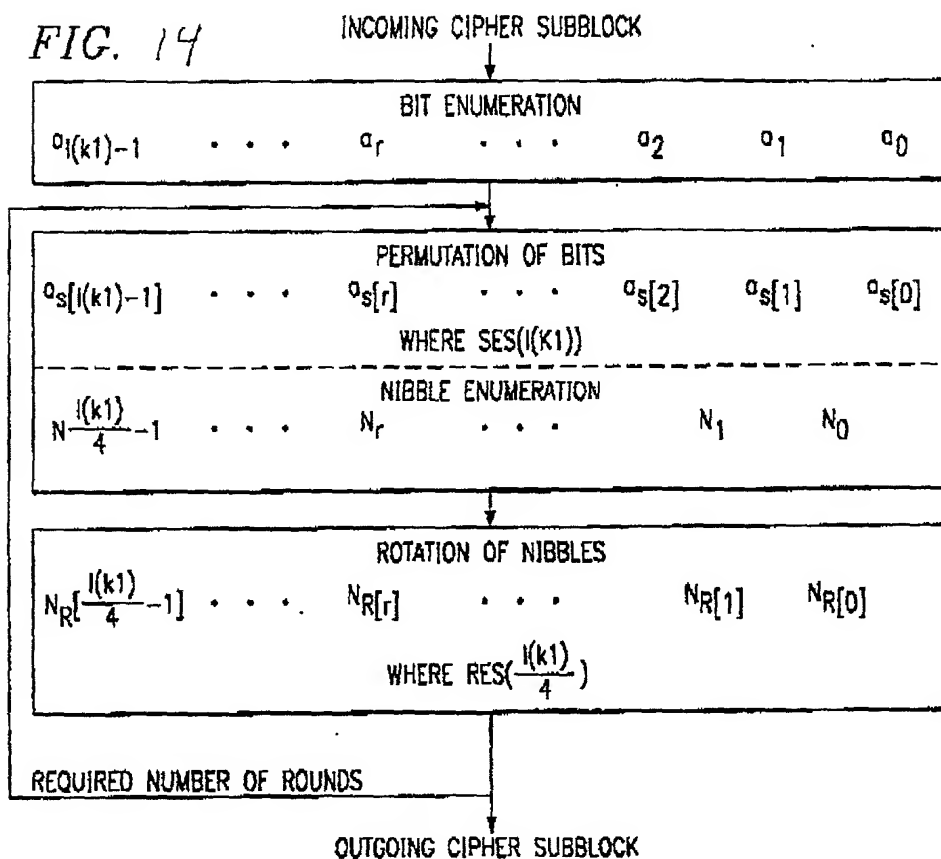


FIG. 14



FOR THE

A4

FIG. 16

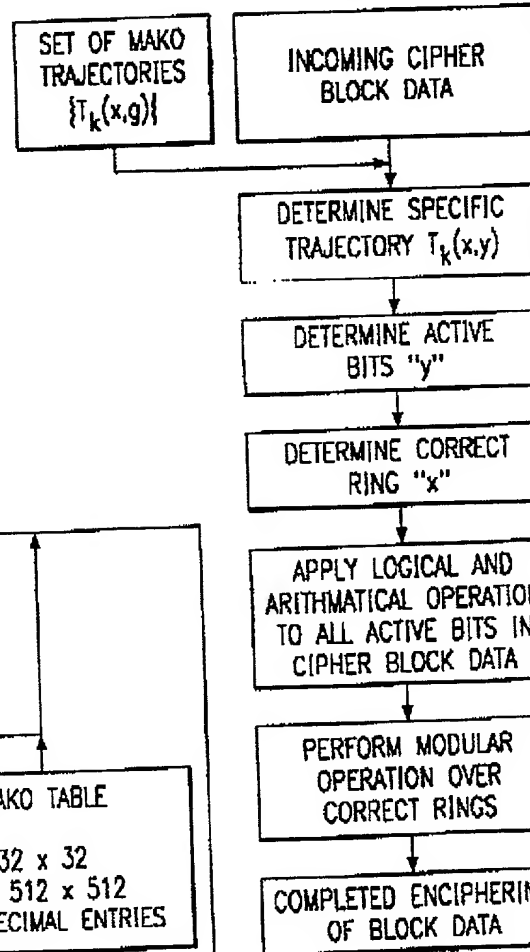
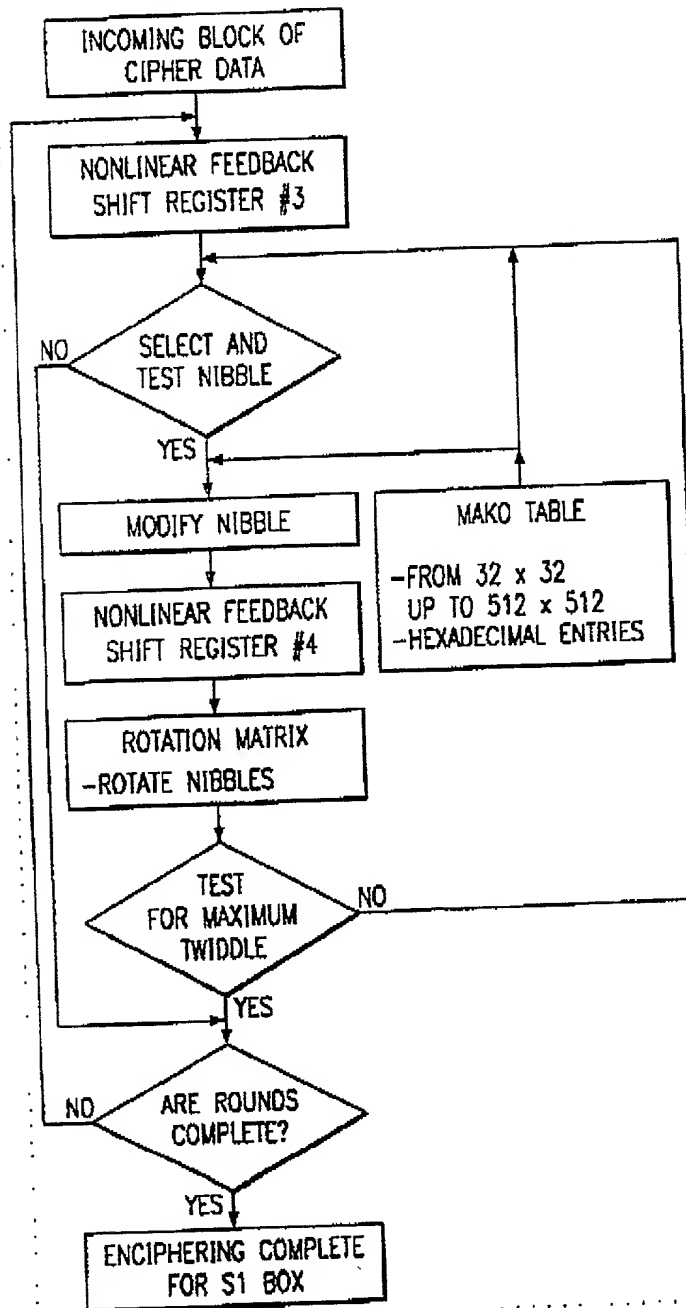


FIG. 15



A4

FIG. 17

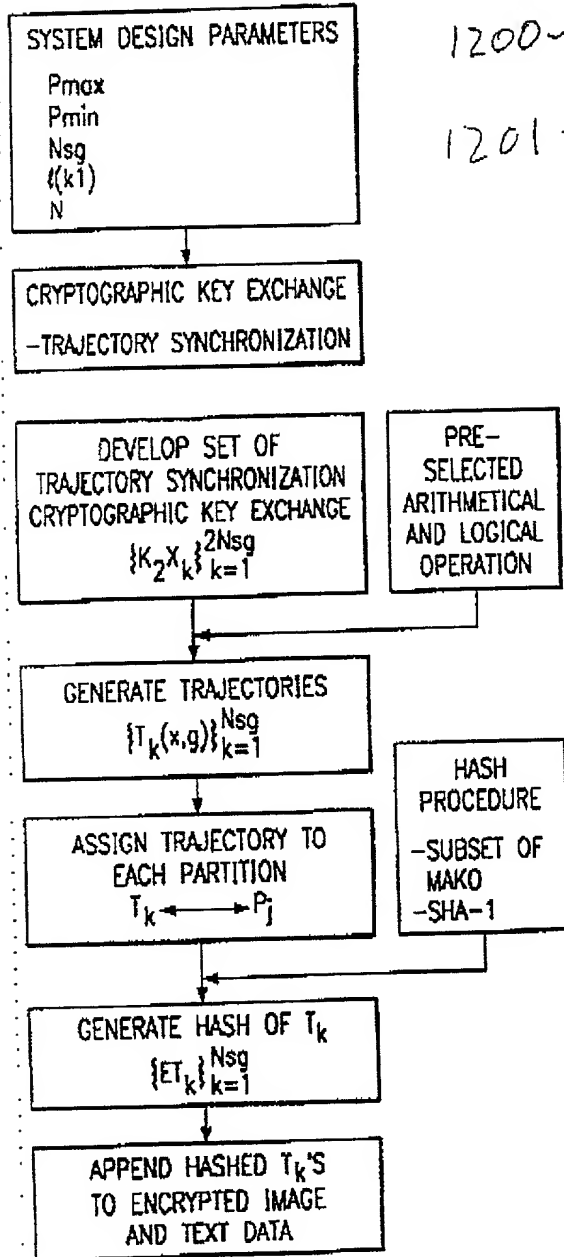
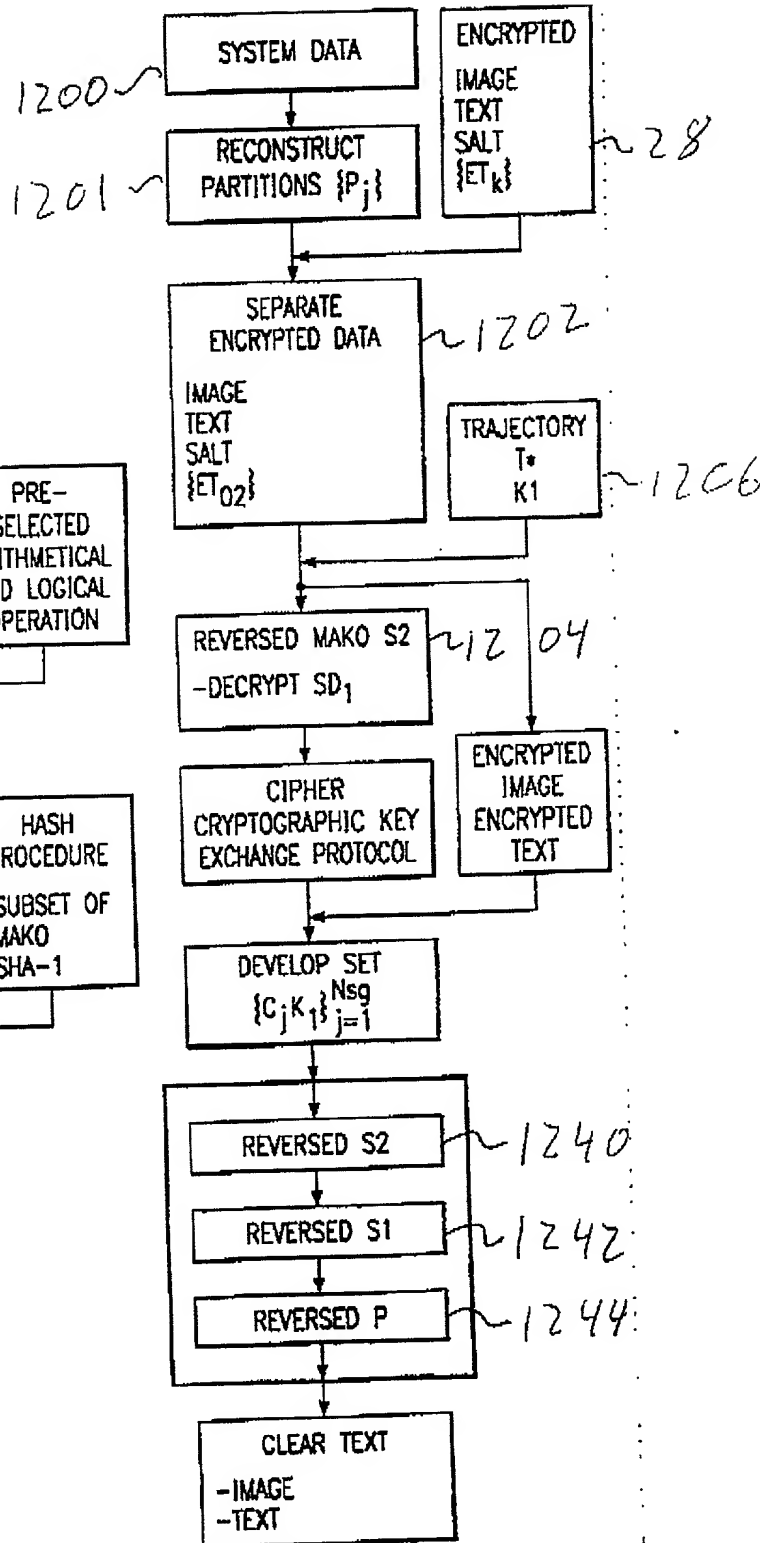


FIG. 18



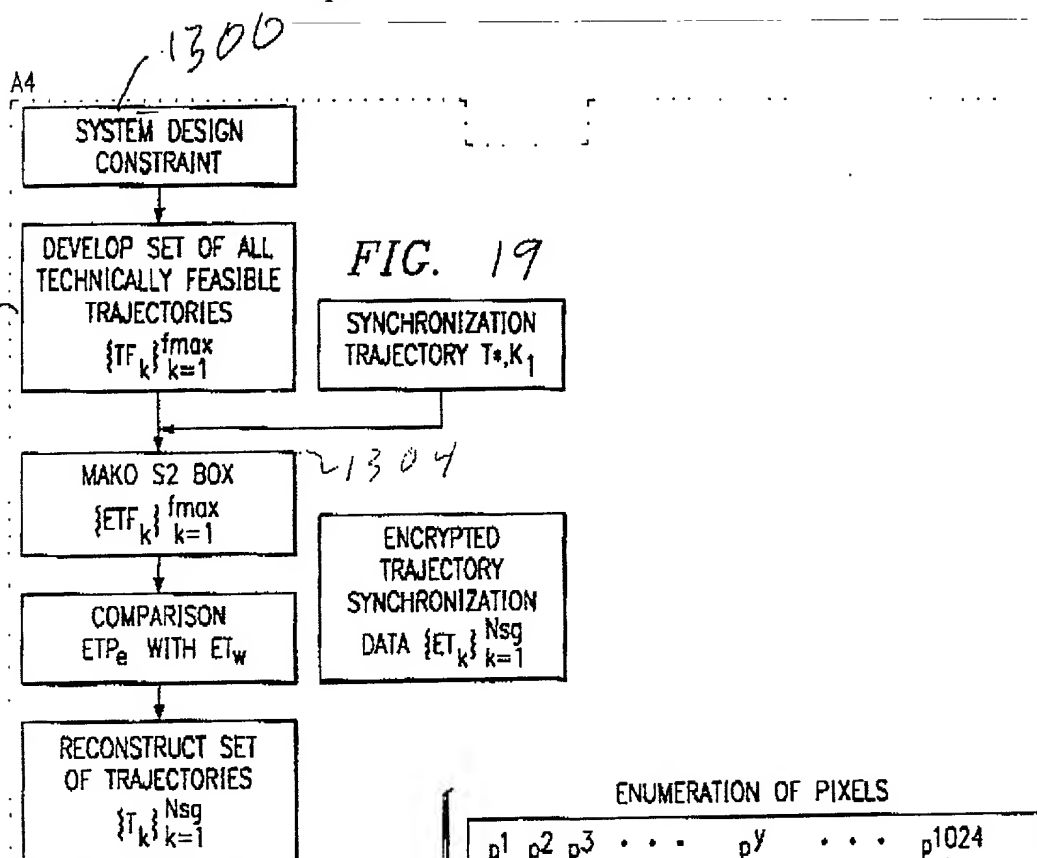
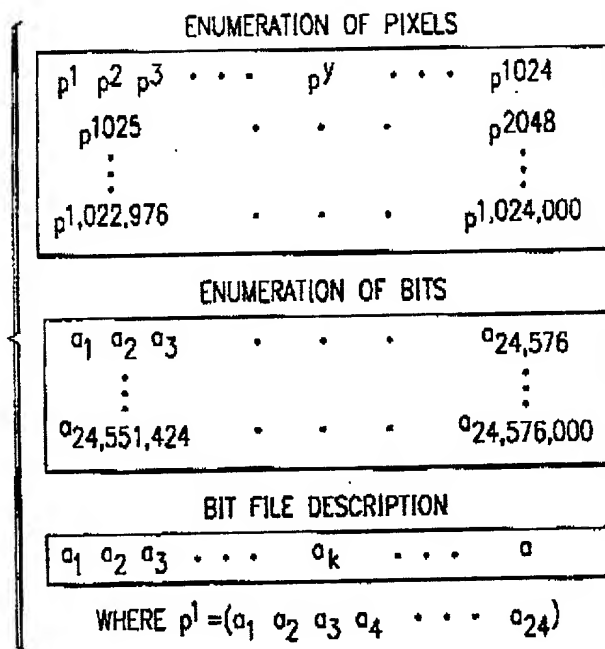


FIG. 21



PARTITION 1	a_1	a_2	...	$a_{8,192}$
PARTITION 2	$a_{8,193}$	$a_{8,194}$...	$a_{16,384}$
	\vdots			\vdots
PARTITION 3000	$a_{24,567,808}$...		$a_{24,576,000}$

FIG. 22

A4

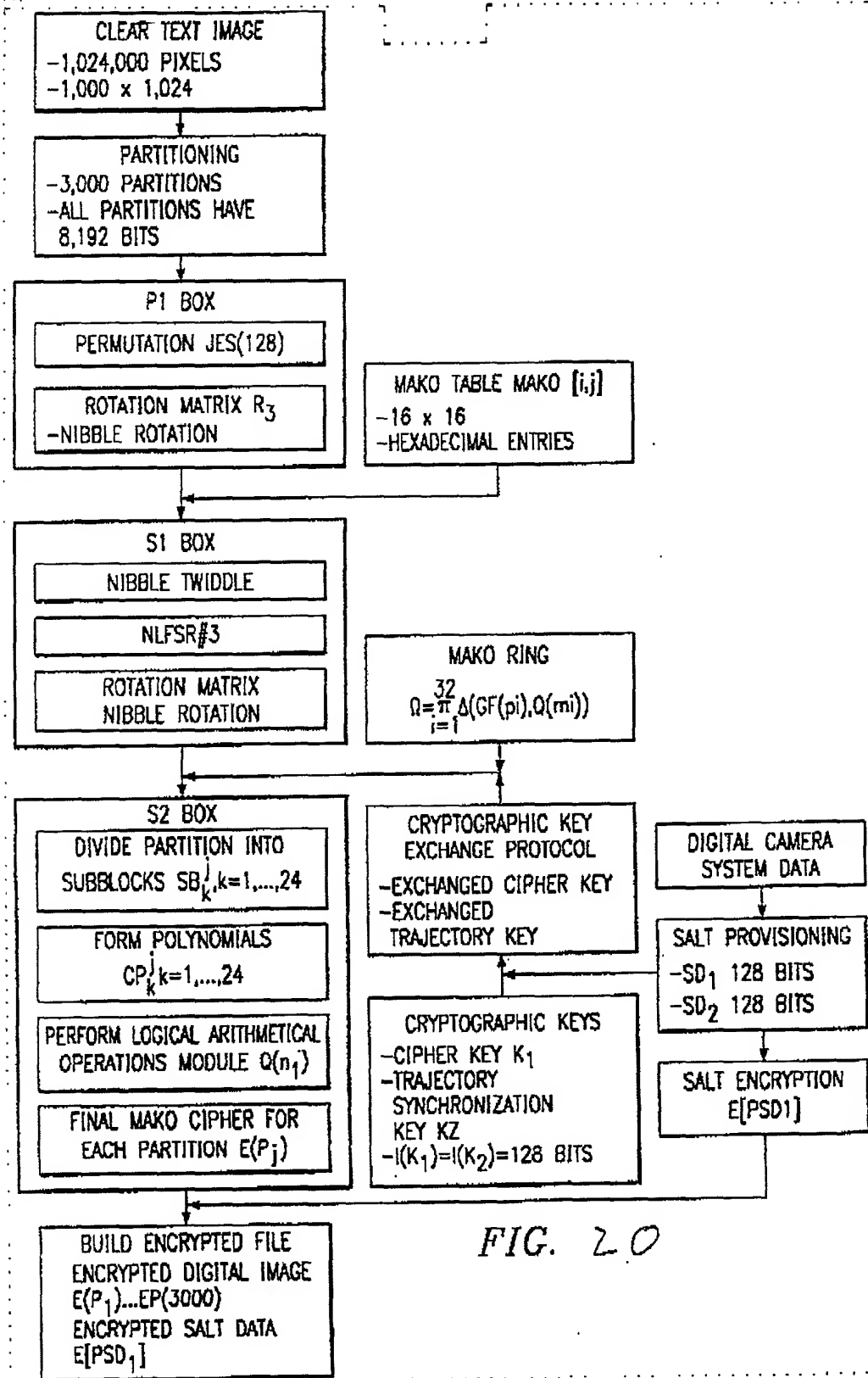
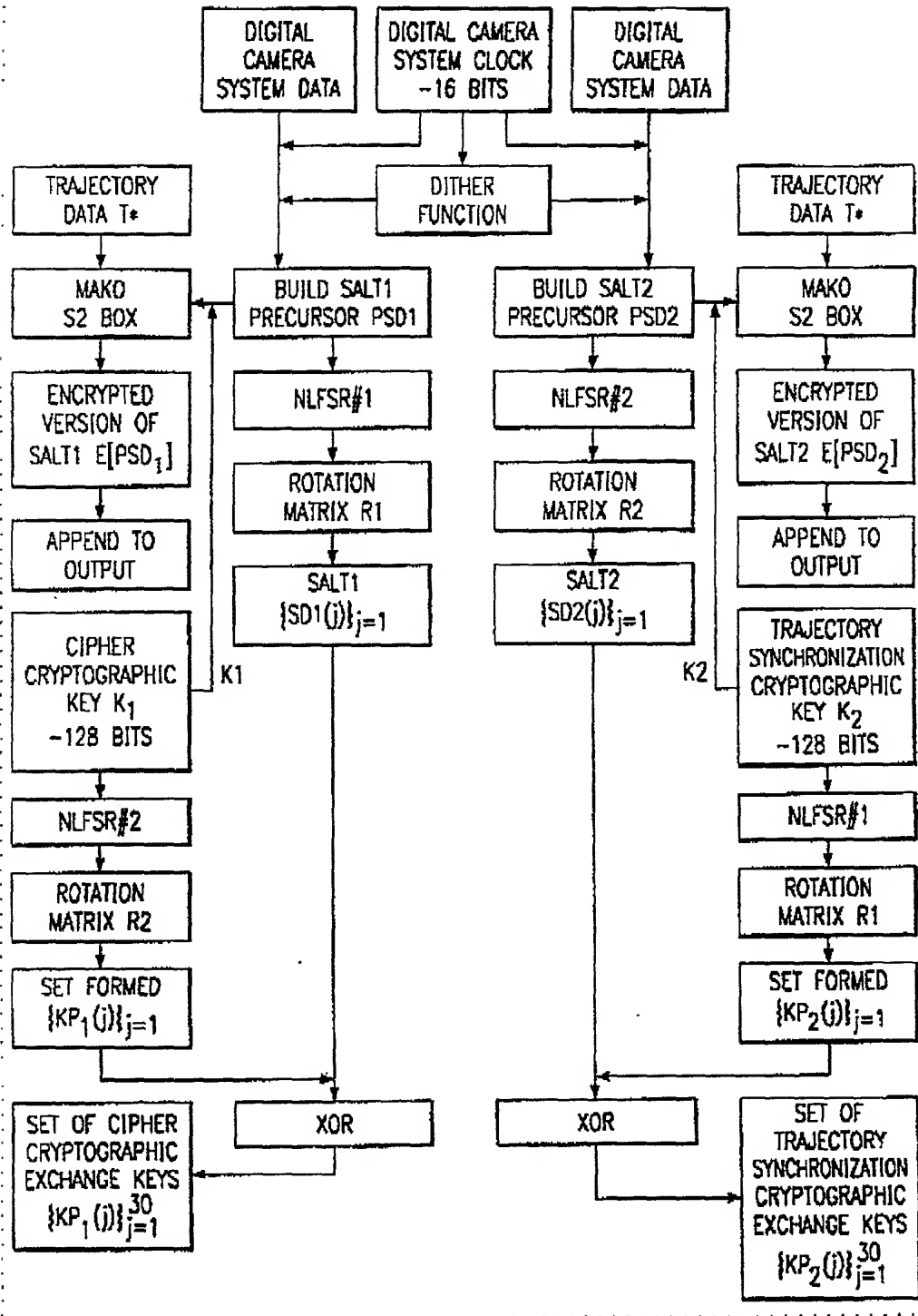


FIG. 20

1009344-1-234104

A4

FIG. 23



A4

FIG. 35

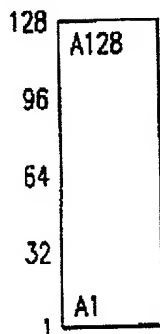


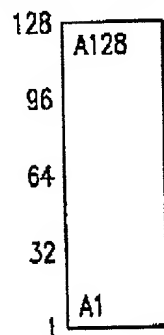
FIG. 33

CURRENT	NEW
R0	R23
R1	R24
R2	R25
R3	R26
R4	R27
R5	R28
R6	R29
R7	R30
R9	R31
R8	R0
R10	R1
R11	R2
R12	R3
R13	R4
R14	R5
R15	R6
R16	R7
R17	R8
R18	R9
R19	R10
R20	R11
R21	R12
R22	R13
R23	R14
R24	R15
R25	R16
R26	R17
R27	R18
R28	R19
R29	R20
R30	R21
R31	R22

FIG. 34

CURRENT	NEW
R0	R13
R1	R14
R2	R15
R3	R16
R4	R17
R5	R18
R6	R19
R7	R20
R9	R21
R8	R22
R10	R23
R11	R24
R12	R25
R13	R26
R14	R27
R15	R28
R16	R29
R17	R30
R18	R31
R19	R0
R20	R1
R21	R2
R22	R3
R23	R4
R24	R5
R25	R6
R26	R7
R27	R8
R28	R9
R29	R10
R30	R11
R31	R12

FIG. 36



INCOMING SUBBLOCK
(128 BITS)

PERFORM LOOP 4 TIMES

PERMUTATION OPERATIONS
(1 128) (2 127) (3 126) . . . (64 65)

ROTATION MATRIX
R₃

OUTPUT DATA

FIG. 24

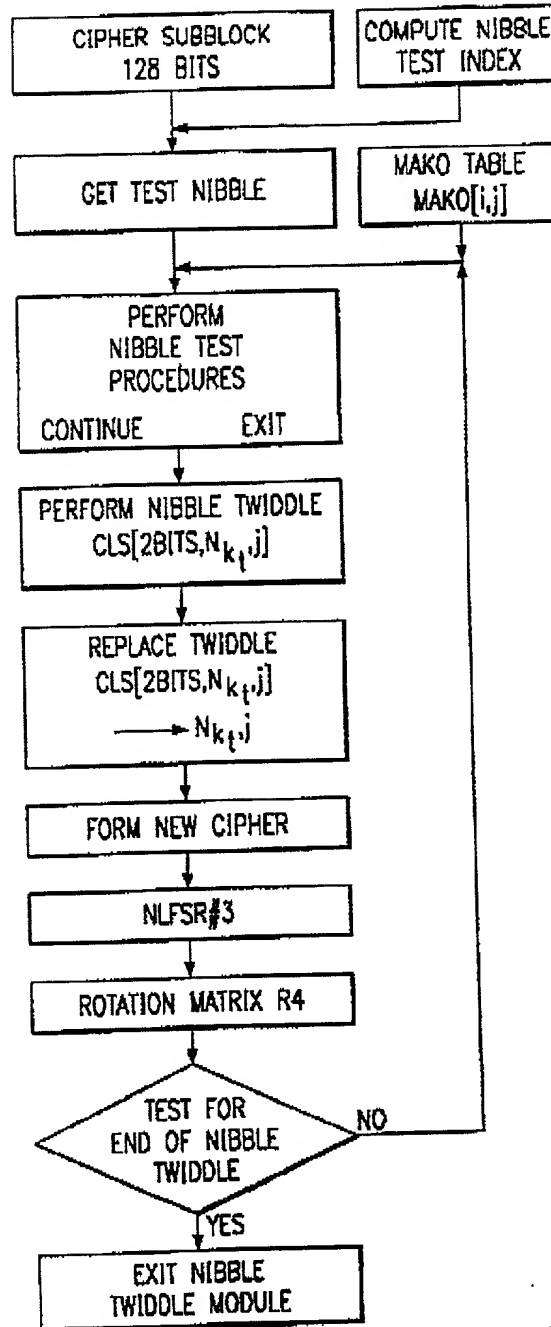
1008344-12401

A4

FIG. 25

CURRENT	NEW
R0	R15
R1	R14
R2	R13
R3	R12
R4	R11
R5	R10
R6	R9
R7	R8
R9	R22
R10	R21
R11	R20
R12	R19
R13	R18
R14	R17
R15	R16
R16	R31
R17	R30
R18	R29
R19	R28
R20	R27
R21	R26
R22	R25
R23	R24
R24	R7
R25	R6
R26	R5
R27	R4
R28	R3
R29	R2
R30	R1
R31	R0

FIG. 26



A4

FIG. 27

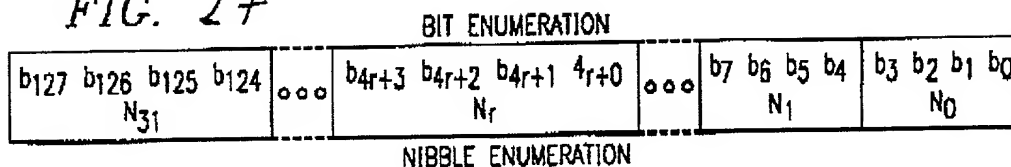


FIG. 32

MAKOTABLE[m_{ij}]=

0f	1f	2f	3f	4f	5f	6f	7f	8f	9f	af	bf	cf	df	ef	
1e	2e	3e	4e	5e	6e	7e	8e	9e	ae	bc	ce	de	ee	fe	0
2d	3d	4d	5d	6d	7d	8d	9d	ad	bd	cd	dd	ed	fd	0d	1
3c	4c	5c	6c	7c	8c	9c	ac	bc	cc	dc	ec	fc	0c	1c	2
4b	5b	6b	7b	8b	9b	ab	bb	cb	db	eb	fb	0b	1b	2b	3
5a	6a	7a	8a	9a	aa	ba	ca	da	ea	fa	0a	1a	2a	3a	4
69	79	89	99	a9	b9	c9	d9	e9	f9	09	19	29	39	49	5
78	88	98	a8	b8	c8	d8	e8	f8	08	18	28	38	48	58	6
87	97	a7	b7	c7	d7	e7	f7	07	17	27	37	47	57	67	7
96	a6	b6	c6	d6	e6	f6	06	16	26	36	46	56	66	76	8
a5	b5	c5	d5	e5	f5	05	15	25	35	45	55	65	75	85	9
b4	c4	d4	e4	f4	04	14	24	34	44	54	64	74	84	94	a
c3	d3	e3	f3	03	13	23	33	43	53	63	73	83	93	a3	b
d2	c2	f2	02	12	22	32	42	52	62	72	82	92	a2	b2	c
e1	f1	01	11	21	31	41	51	61	71	81	91	a1	b1	c1	d
e0	00	10	20	30	40	50	60	70	80	90	a0	b0	c0	d0	f0

10028344.123104

A4

FIG. 28

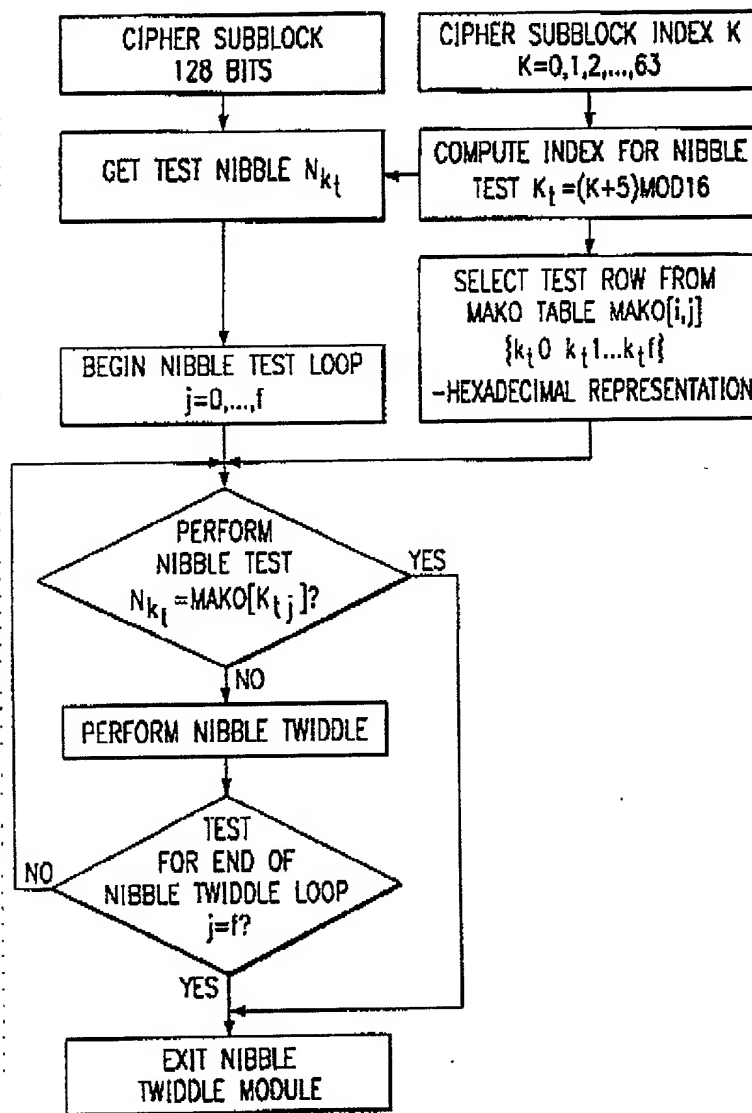
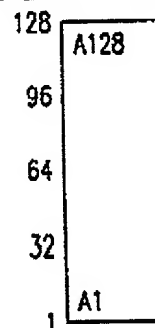


FIG. 37

CURRENT	NEW
R0	R15
R1	R14
R2	R13
R3	R12
R4	R11
R5	R10
R6	R9
R7	R8
R9	R22
R10	R21
R11	R20
R12	R19
R13	R18
R14	R17
R15	R16
R16	R31
R17	R30
R18	R29
R19	R28
R20	R27
R21	R26
R22	R25
R23	R24
R24	R7
R25	R6
R26	R5
R27	R4
R28	R3
R29	R2
R30	R1
R31	R0

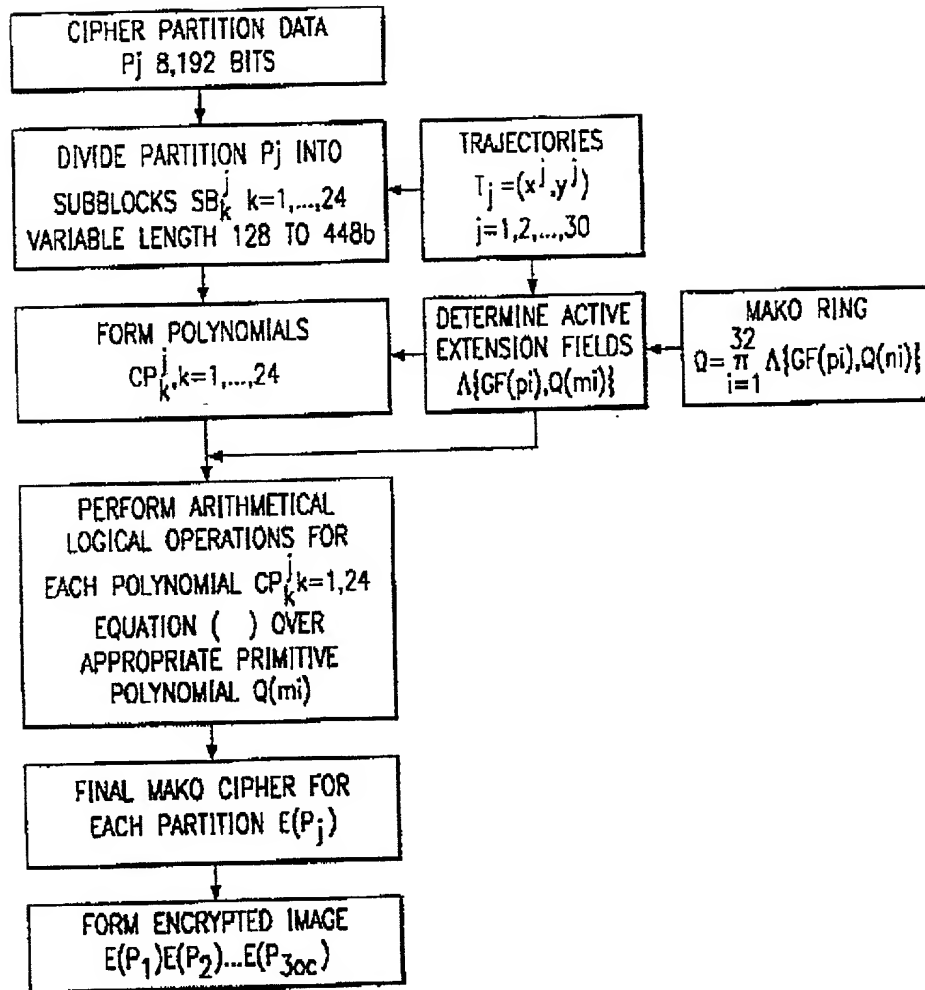
FIG. 29



10026341.123404

A4

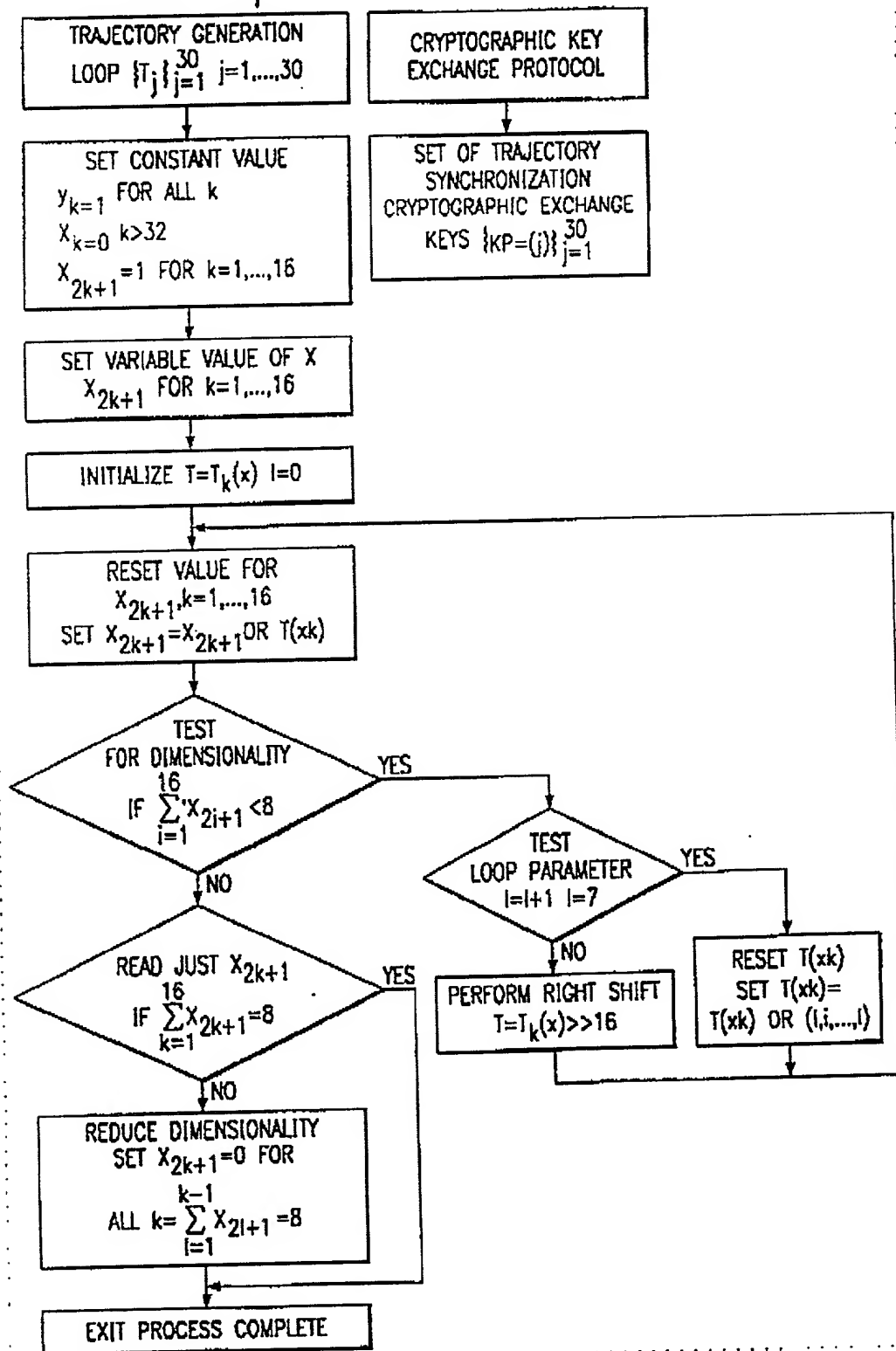
FIG. 30



1006944-1001

A4

FIG. 31



100263441-133404